Security requirements analysis based on security and domain ontologies

Amina Souag[1], Camille Salinesi[1], Isabelle Wattiau[2]
[1] CRI, Paris 1 Sorbonne University
{Amina.Souag, camille.salinesi}@malix.univ-paris1.fr
[2] CEDRIC-CNAM & ESSEC Business School, France
isabelle.wattiau@cnam.fr

Security is the discipline concerned with protecting systems from a wide range of threats (malice, error or mischief) that break the system by exploiting a vulnerability, i.e. a property of the system or its environment that, when faced with particular threats, can lead to failure[5] . Security is a multi-faceted problem; it is as much about understanding the domain in which systems operate as it is about the systems themselves. While developing security facilities such as encryption, identity control, or specific architectures is important, our attention should be drawn at looking into the sociotechnical context in which target systems will operate and threats that may arise and their potential harm, so as to uncover security requirements. Recent research has argued about the importance of considering security at the early stages of the information systems development process, and especially the need to consider security during RE.

An ontology, in the field of knowledge representation, is most often defined as "a representation of a conceptualization"[1]. It should represent a shared conceptualization in order to have any useful purpose [2]. Ontologies are useful for representing and interrelating many types of knowledge. Several security ontologies have been proposed [3]. Domain ontologies are formal descriptions of classes of concepts and relationships between these concepts that describe a given domain.

Our previous experience with RITA [4] a requirements elicitation method that exploits a just one threat ontology, was that "being generic, the threats in the RITA ontology are not specific to the target [bank] industry" (the case study was in the banking sector). Experts involved in the evaluation complained about "the lack of specificity of the types of threats to the industry sector and the problem domain at hand". The problem that remains open is therefore that we need to exploit both security knowledge and domain knowledge to guide the elicitation of domain-specific security requirements. Our research question is "how to combine the use of security ontologies and domain ontologies to guide requirements elicitation efficiently?"

This paper presents an ongoing research project that aims to develop a method that explores the use of security and domain ontologies for SRE. The approach is generic in the sense that different security ontologies and different domain ontologies can be used with it. However it is domain specific when it is applied in the sense that during its application only one domain ontology is used.

Our method guides the discovery of security requirements for a specific domain. This process handled by a series of heuristic production rules that, starting from high level security requirements, produce a security requirements specification. Figure 1 shows an overview of our method. There are two sub-sets of rules. The first set of rules handles domain-specific analysis. The second set of rules performs a security specific analysis. Each set of rules exploits different ontologies: respectively domain ontologies and security ontologies. In order to be able to handle different security and domain ontologies, the rules were specified with so-called “upper ontologies”, that handle concepts that are (a) common to most ontologies, (b) sufficiently high level to abstract many other concepts in the specific ontologies, and (c) more importantly that represent an important subject of interest for the method.

The requirements definition process starts with the elicitation step, where stakeholders express their needs about security in non-formal sentences. Then an analysis stage is carried out to discover more requirements and express these needs in a semi-formal requirement.

During the elicitation step, an initial I* requirements model is first constructed from the stakeholders' needs and concerns expressed about security at the beginning of the project. At this stage, the analyst defines initial actors, resources, and especially security goals (integrity, confidentiality, traceability...) During the security requirements analysis stage, the production rules will exploit the security-specific ontology to discover threats, vulnerabilities, countermeasures, and resources, and thus enrich the requirements model by adding new elements (malicious tasks, vulnerability points...). During the domain specific security requirements analysis stage, another set of rules explores the domain ontology to improve the requirements model with resources, actors and other concepts that are more specific to the domain at hand; for instance: thieves in the banking domain, hijackers in the aeronautic domain, pirates in the maritime domain, etc.

The originality of the method lies: (a) in the fact that the combination of security and domain ontologies is not achieved a priori, but at runtime, while the method is applied, and (b) in the genericity of the method, in the sense that it is designed to be used with any pair of security and domain ontologies, as long as they embed some expected knowledge.

Our preliminary evaluation conducted through a small, but real, case study and through critical analysis by three experts (domain, security, requirements engineering, respectively). The evaluation shows that the method provides a good balance between the genericity with respect to the ontologies (which do not need to be selected in advance), and the specificity of the elicited requirements with respect to the domain at hand.

References

[1] T. R. Gruber, « Toward principles for the design of ontologies used for knowledge sharing? », Int. J. Hum.-Comput. Stud., vol. 43, nº 5‑6, p. 907‑928, nov. 1995.

[2] G. Dobson et P. Sawyer, Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web. In: Dependable Requirements Engineering of Computerised Systems at NPPs. 2006.
[3] S. Fenz et A. Ekelhart, « Formalizing information security knowledge », in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, New York, NY, USA, 2009, p. 183–194.
[4] C. Salinesi, E. Ivankina, et W. Angole, « Using the RITA Threats Ontology to Guide Requirements Elicitation: an Empirical Experiment in the Banking Sector », in Managing Requirements Knowledge, 2008. MARK '08. First International Workshop on, 2008, p. 11 - 15.
[5] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, 2010.